



Latest Trends in Mobile Security

By
M K Chaithanya
C-DAC Hyderabad

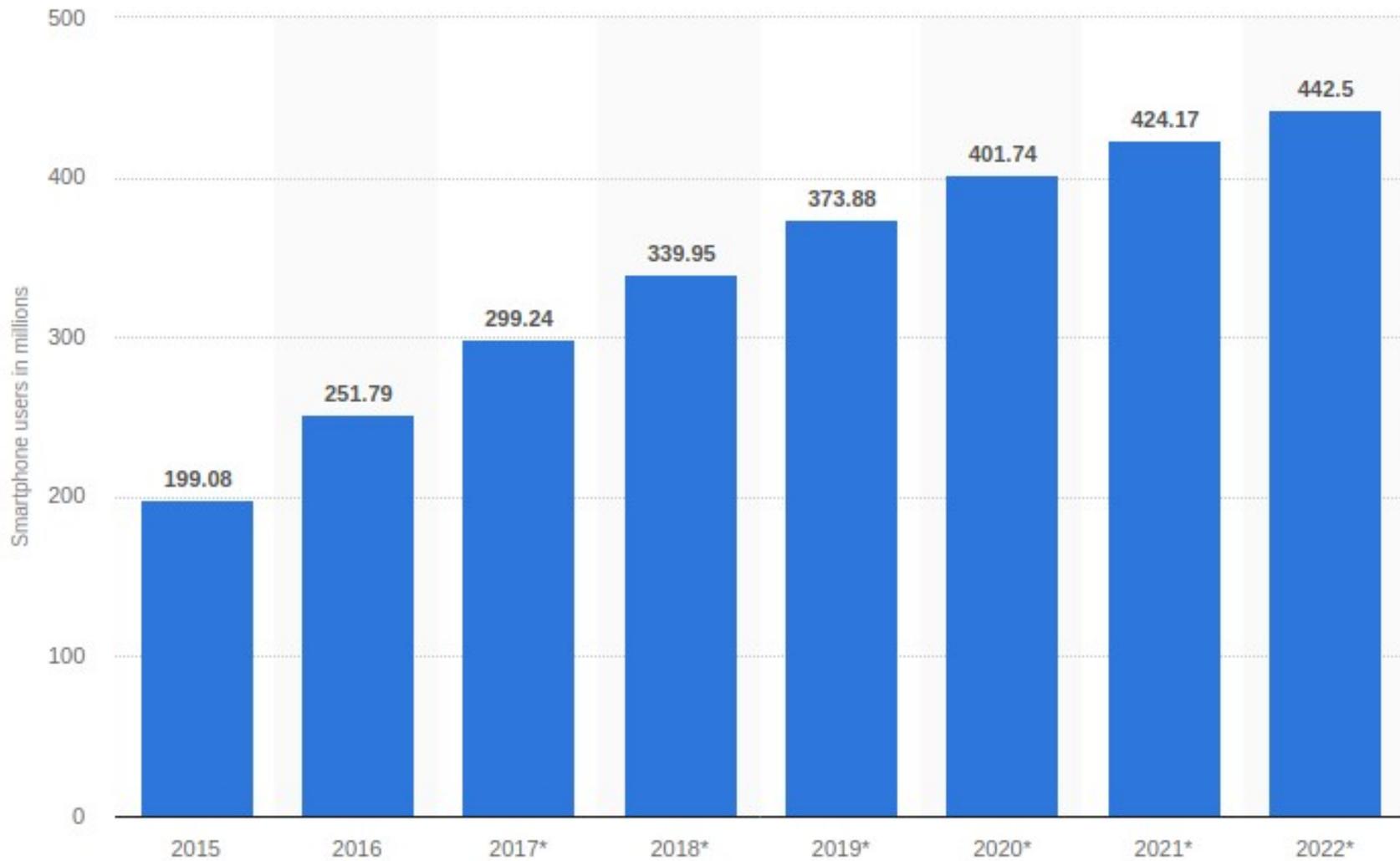
- Introduction
- Statistics of Mobile Usage
- Current State of Mobile Security
- Recent Attacks
- Various Mobile Threats
- Security & Privacy Configurations
- Security Tips

- Mobile devices have revolutionized the way we communicate, we surf the internet, we do payments, we do gaming and many more
- They have the capability to perform the functionality of a camera, calculator, barcode reader, credit card scanner, USB thumb drive, eBook reader, audio recorder and many more

- This multi function capability of the device along with the cost and mobility factor has made mobile devices an important part of personal and business life of people and organizations
- This has led to tremendous increase in the usage of mobile devices in the country
- Now a days, mobile devices have become an important part of personal and business life of people and organizations

Current State of Mobile Device Usage in the Country

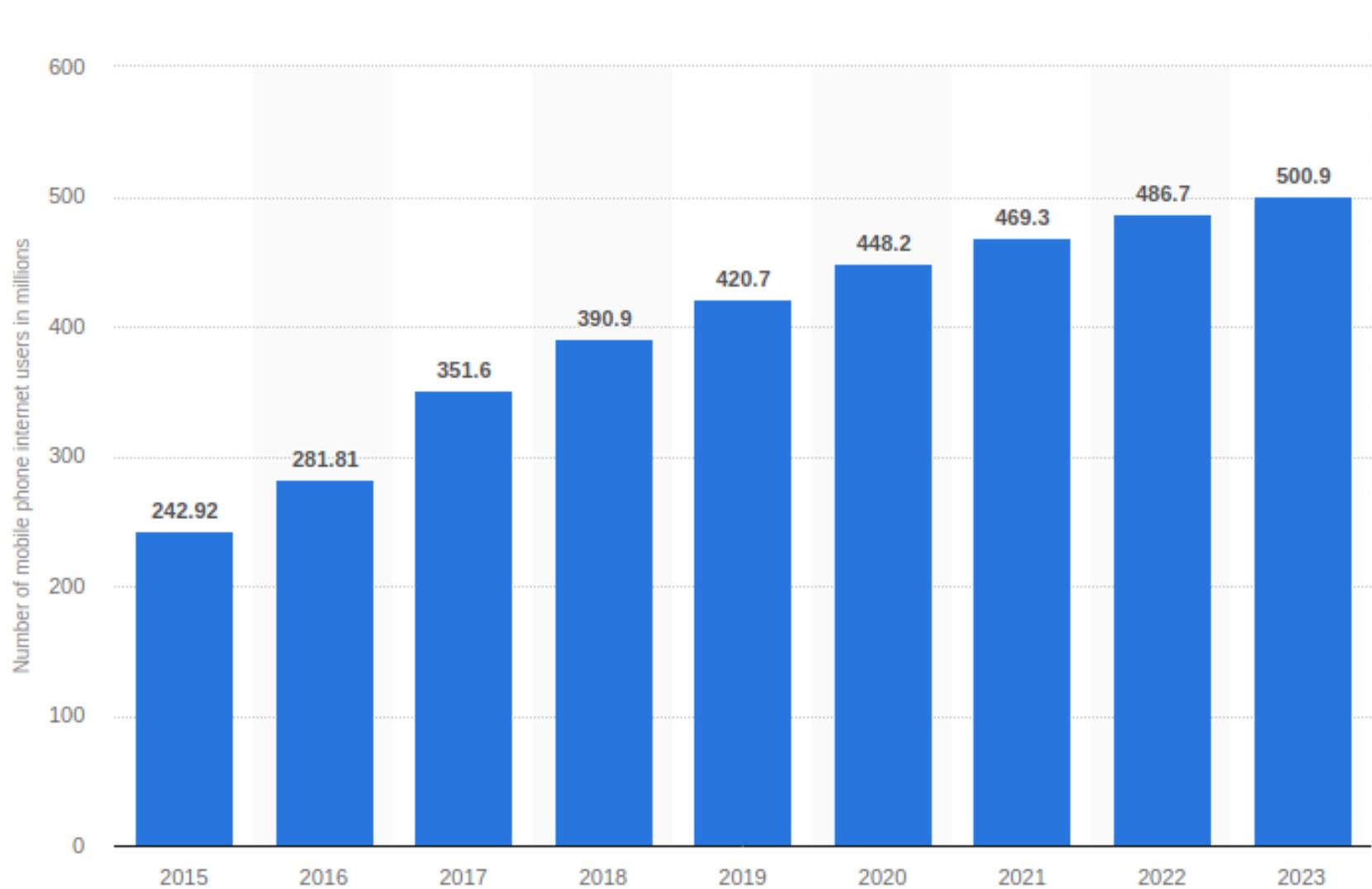
Smart Phone users in India



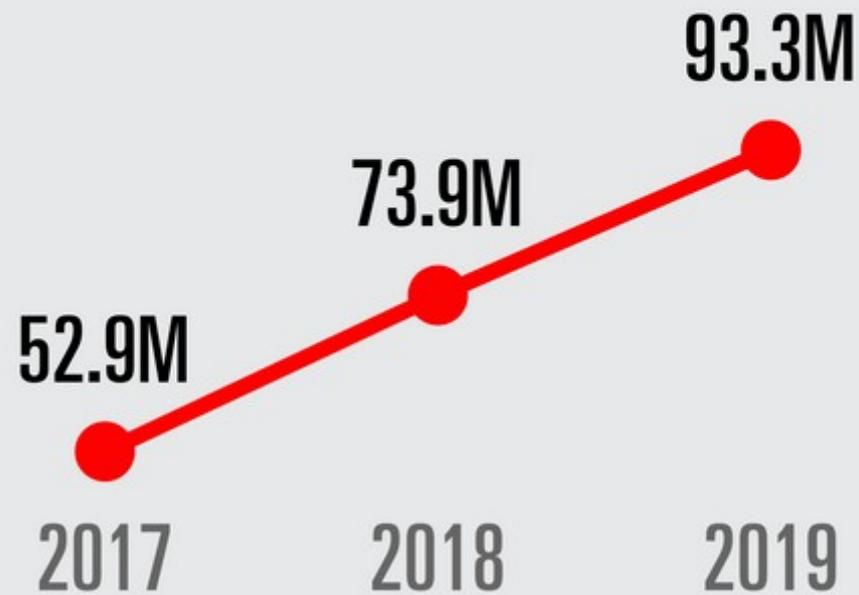
Current Statistics

- No. of smart phone users have already crossed 500 mn in 2019 itself
- Current predictions say that the no. of smart phone users would cross 850 mn by 2022

Mobile Internet Users in India



How Many People in India Use Mobile Payments





Major cause for increase in mobile threats

- This tremendous increase in the usage of mobile devices has led to huge amounts of personal and business related data being stored and accessed on the mobile devices
- This same reason has become the motivation for hackers and attackers to target these devices which have become mini hubs of rich data

- Android is by large the most widely adopted mobile platform in the world powering over 2.5 billion devices across the globe
- Main reason for the popularity of Android is it's openness & strong eco-system
 - OEMs
 - Developers
 - Freelancers
 - Users

- This increased popularity of Android and growth in eco-system has attracted more number of malicious developers into the ecosystem
- So, malicious developers have become the extended arm of the Android eco-system

Current State of Mobile Security in the Country



Smartphones became hotspots of cyber attacks in India

- If you are thinking that only large critical infrastructure and big corporations would be targeted for cyber attacks, you are wrong
- In India, smartphones, the device that most people now carry in their pockets, have become a very large attack centre, said a top security expert at Check Point



Cyber Security Incidents from 2016 to October 2019

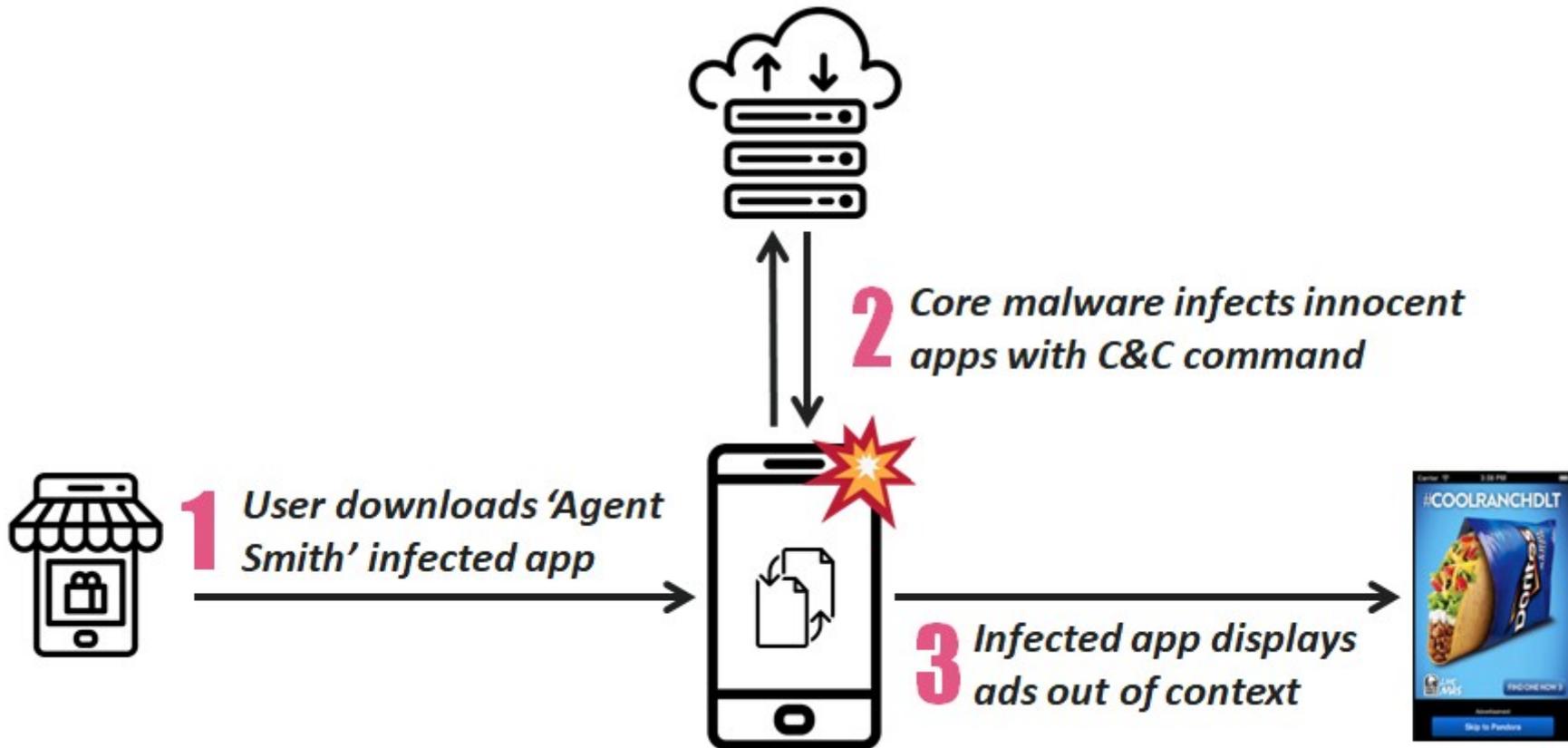


- 2016 – 50,362
- 2017 – 53,117
- 2018 – 2,08,456
- 2019 (Till Oct) – 3,13,000 +

Android Malware silently infects 25mn users in India



- A new mobile malware targeting Android users across India can hijack legitimate apps to deliver malicious code, researchers have warned
- The attack, dubbed 'Agent Smith', has reportedly affected around 25 million device users without their knowledge
- The three-stage attack is exploited to deliver advertisements for financial gain
- The malware is downloaded onto the phone knowingly, usually via a "barely functioning photo utility, games, or sex-related" apps



Some Facts

- Bulk of the mobile phones in India are running a very old version of Android
- Mobile hardware is not manufactured in the country nor is the software that runs on it
- Even the anti-malware solutions being used in the country are neither designed nor developed in the country
- A report from Qualcomm says wallets and mobile banking applications in India are not using hardware level security which can make online transactions more secure

Some Facts

- There are numerous fake banking applications and wallets detected in the Google playstore targeting victims in India which mimic the names or graphic design specifications of existing apps
- Insecure mobile browsers are posing a serious threat to the security and privacy of mobile users in the country
- Anti-Virus companies such as Quick-Heal, Kaspersky etc are extracting lot of analytical information from the users
- There is a possibility of increased threat landscape in the country with the introduction of 5G

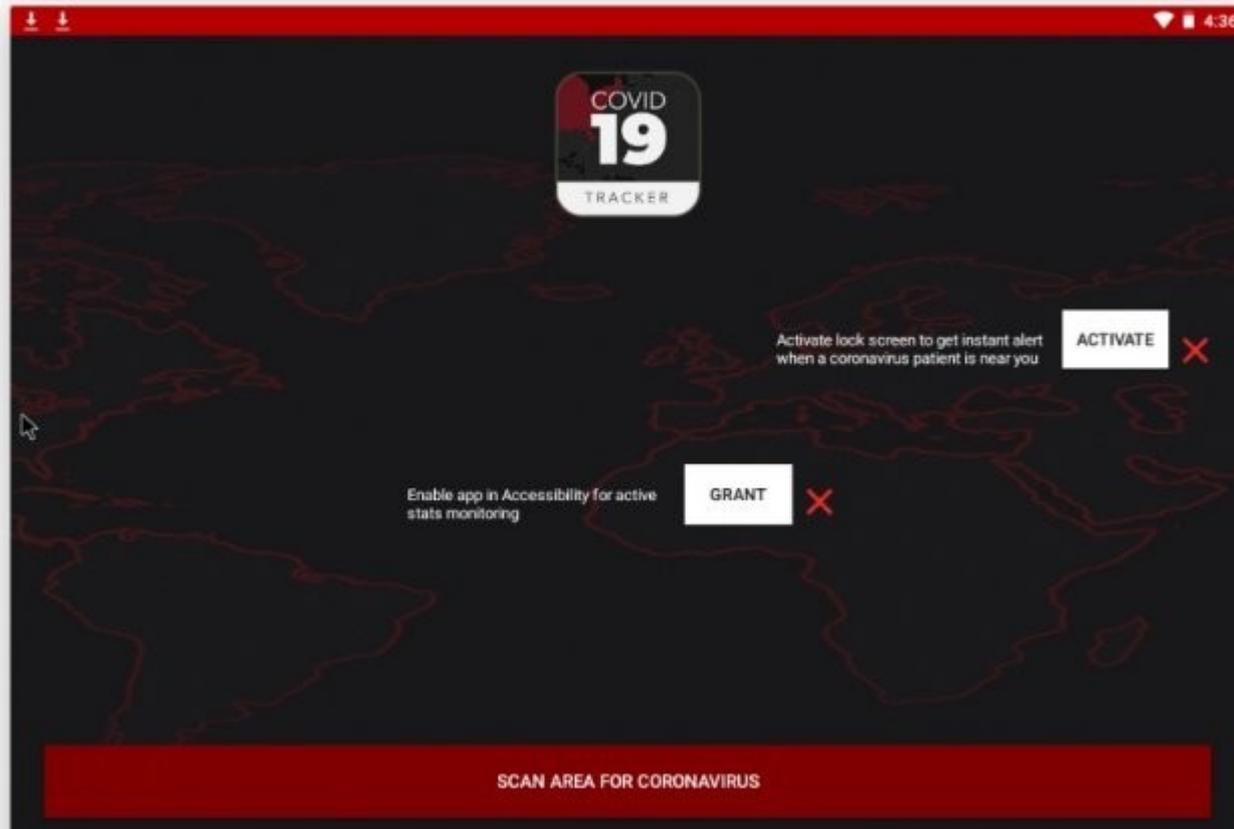
Some Recent Attacks



- Hackers are misusing COVID-19 global pandemic to prey on naive users to steal financial credentials
- They have developed a malicious software named Coronavirus tracking Android app
- The COVID19 Tracker app is available for download on the website
- If any user comes to the site, he/she will be asked to download the Android app for the map

- It says to offer the information on the spread of the pandemic in addition to country-wise statistics of COVID-19 infections, recoveries and fatalities
- Once installed, the Coronavirus app, which houses ransomware 'CovidLock' takes full control of the phone and blocks the user from opening the screen lock
- It demands a ransom of \$100 in bitcoins to the victims
- If they don't oblige within 48 hours, it warns of permanently delete all the contacts, videos, images, messages and other personal information on the phone

Malicious COVID19 Tracker App





Whats App Zero-Click Spyware Attack

- A vulnerability had been discovered that let attackers install spyware on iPhones and Android phones simply by placing a WhatsApp voice call to the user's smartphone
- What's notable about the WhatsApp attack is that it was a “zero-click” or “no click” attack.
- That means the spyware was able to be installed on a smartphone by the attacker simply placing a WhatsApp voice call to the phone.



Whats App Zero-Click Spyware Attack

- It does not matter if the call was answered or not—a target did not have to open any message, answer the call, or click on any link
- The spyware was allegedly created by the Israeli cyber surveillance company NSO Group.
- The secretive group creates spyware it sells to governments and law enforcement agencies around the world that allows them to take almost complete control of a device

Facebook's Data Deals

- Facebook's data deals are under criminal investigation
- For years, Facebook gave some of the world's largest technology companies more intrusive access to users' personal data than it has disclosed, effectively exempting those business partners from its usual privacy rules, according to internal records and interviews
- This emphasizes how personal data has become the most prized commodity of the digital age, traded on a vast scale by some of the most powerful companies

Contd..

- Facebook allowed Microsoft's Bing search engine to see the names of virtually all Facebook users' friends without consent
- The records show, and gave Netflix and Spotify the ability to read Facebook users' private messages
- The social network permitted Amazon to obtain users' names and contact information
- A political consulting firm, Cambridge Analytica, improperly used Facebook data to build tools that aided President Trump's 2016 campaign in US



Uber mishandles user's and driver's data

- San Francisco-based firm failed to closely monitor employees who had access to consumer and driver data
- It failed to deploy “reasonable measures” to secure personal information it stored on a third-party cloud provider’s servers
- Uber is also being sued by a former employee who claims he was fired after blowing the whistle about insecure data practices at the company

- Hidden Apps
- Mobile Phishing
- Fake Mobile Apps
- Malware
- Spyware
- Adware
- Ransomware
- IoT Threats
- WiFi-Threats
- Data leaks
- Misconfiguration of devices

Fake Apps

- Fake mobile applications are applications that mimic the look and/or functionality of legitimate applications to trick unsuspecting users to install them
- Primary motto of Fakeapps include
 - Stealing of
 - Credentials
 - Financial Data
 - Business Data
 - Other Sensitive Data
 - Display of ads for revenue



How fake applications are built

- Built for a popular brand that doesn't have an application of its own
- Cloning of existing applications and adding malicious code by tampering and repackaging



- Hosted on third-party app stores
- Circulated through social engineering campaigns
- Official app stores such as Google Play stores
- emails and SMS messages that appear to be from bank, credit card company or other brands
- As a notification for security updates

- Number of app downloads
 - A wildly popular app is a sign of a good app
- App reviews
 - Often short and generic reviews could be a sign of fake application
- Developer of the application
 - The more apps that developer has created, the higher the chance that the developer is real
- Visual things such as spelling errors, logos of poor quality and unbalanced or poorly formatted interfaces are clues that the app may be fake



Some recent fake apps detected



- 28 Fake Apps removed from Google Play Store post Quick Heal Security Lab reports
- These apps do not have any legitimate functionality related to App name
 - Credit card process
 - description on play store is “provide credit card process” but in the actual application there is no information related to the credit card process
 - Home Loan Advisor
 - description on play store is, “Gives advice for home loan” but in the actual application there isn’t any information related to home loan advice
- All apps are found to be developed by same developer

Mobile Phishing

- **If You Can Raed Tihs, You Msut Be Raelly Smrat**
- *"Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttar in waht oredr the ltteers in a wrod are, the olny iprmoatnt tihng is taht the frist and lsat ltteers be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe."*

- Phishing attacks remain an effective method of stealing credentials and identities, distributing malware, eliciting fraudulent payments etc.
- Research shows that a new phishing site is launched every 20 seconds
- 87% of successful mobile phishing attacks take place outside of e-Mail
- 60% of mobile phishing attacks occur over HTTPS

- Phishing is also becoming impossible to detect visually.
- Double-checking the address bar for suspicious URLs used to be an easy way to catch a spoof domain
- But now attackers use free services like “Let’s Encrypt” to gain SSL certification for malicious phishing sites
 - <https://letsencrypt.org/>

Hidden Apps

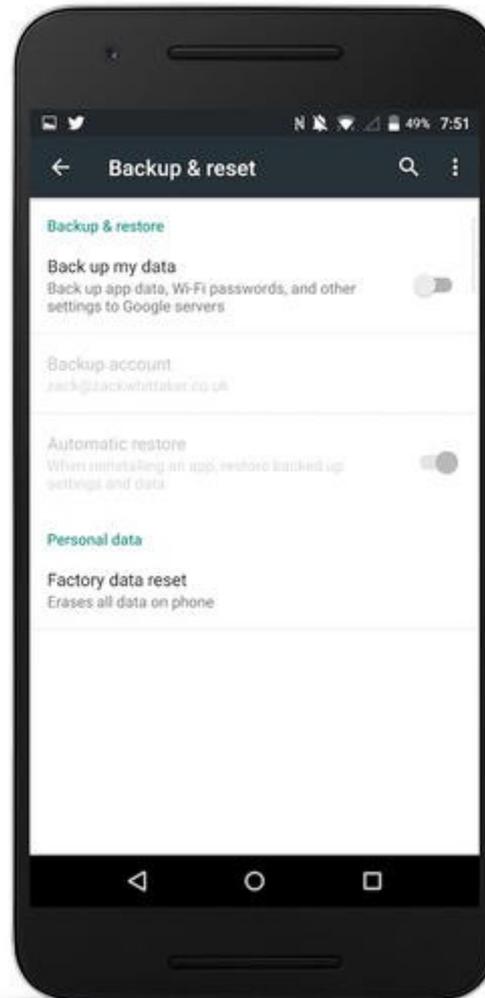
- Hidden apps hide their existence on victim's devices by removing their icons from the home screen and perform malicious activities
- Hidden apps are the most active mobile threat category in 2019
- Thousands of apps are actively hiding their presence after installation, making them difficult to locate and remove while annoying victims with invasive ads

- Criminals are tricking users into installing adware on their devices that redirects them to a range of different ad types and topics
- Digital ad revenue comes from raw numbers—screens displayed and clicks captured
- Fraudulently increasing these numbers is becoming a very popular technique

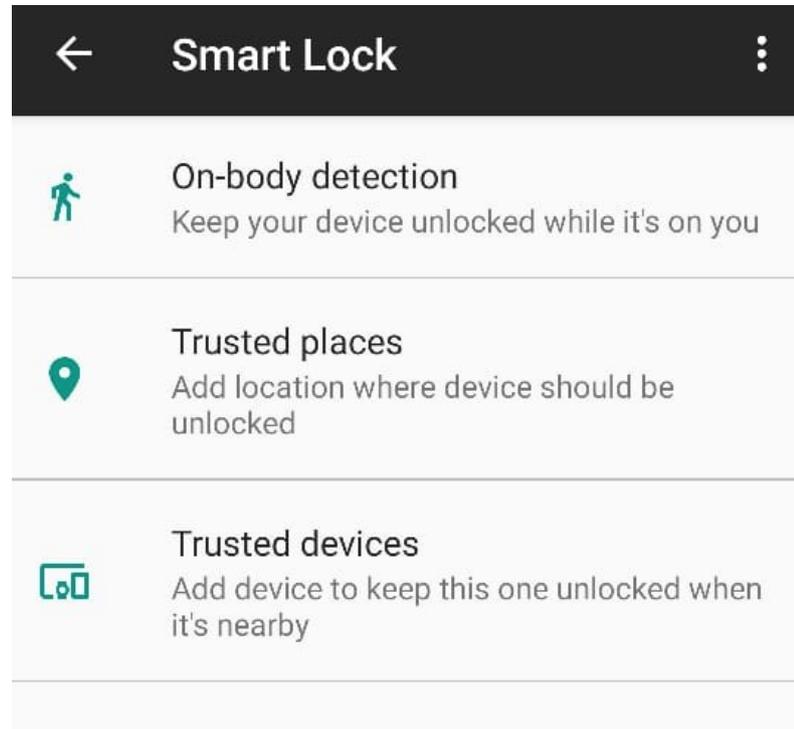
- Masquerades as genuine apps, with similar names and icons, or apps with basic functionality
- Changes icon to hide after installation
- Redirects user to various types of ads and collects user data

Some Important Security & Privacy Configurations in Android

- The best way to keep your Android phone from sending your personal data to its servers is to turn off backup
- The downside is if you lose your phone, you may lose your data
- But you always have the option to manually back-up to your home computer
- Go to **Settings** then **Backup & Reset**, where you can switch off the option to **Back up my data**



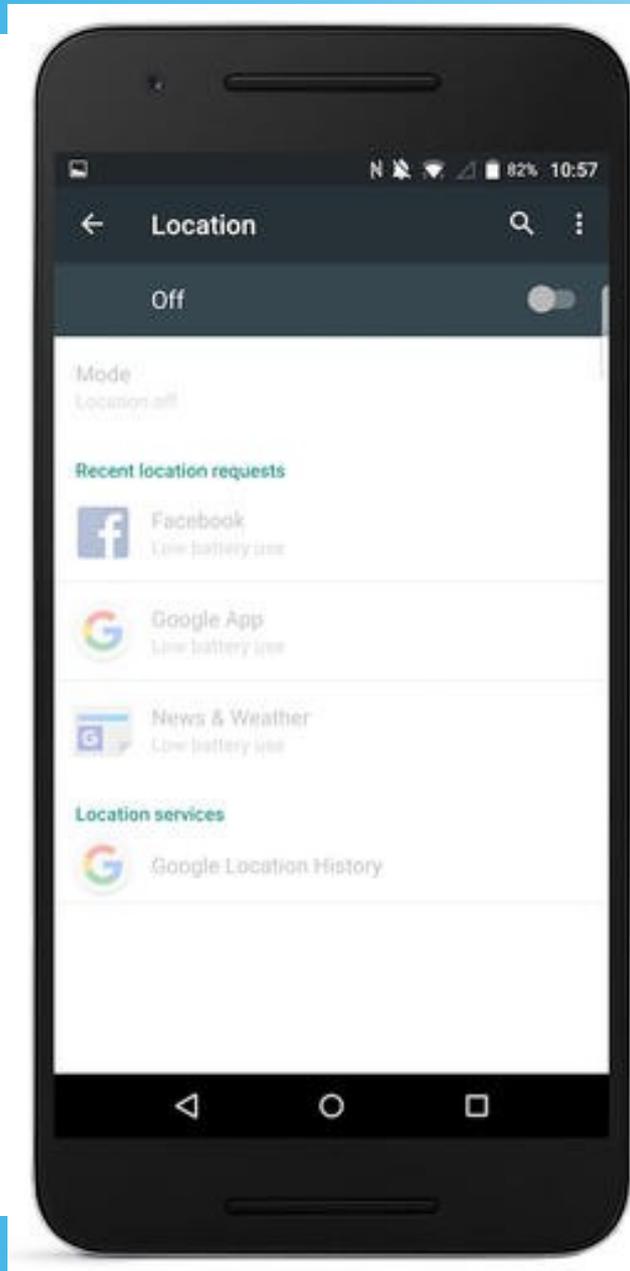
- Smart Lock aims to keep your data secure without taking a convenience hit
- Go to **Settings** then **Device & Privacy**, where you can switch on/off the option to **Smart Lock**



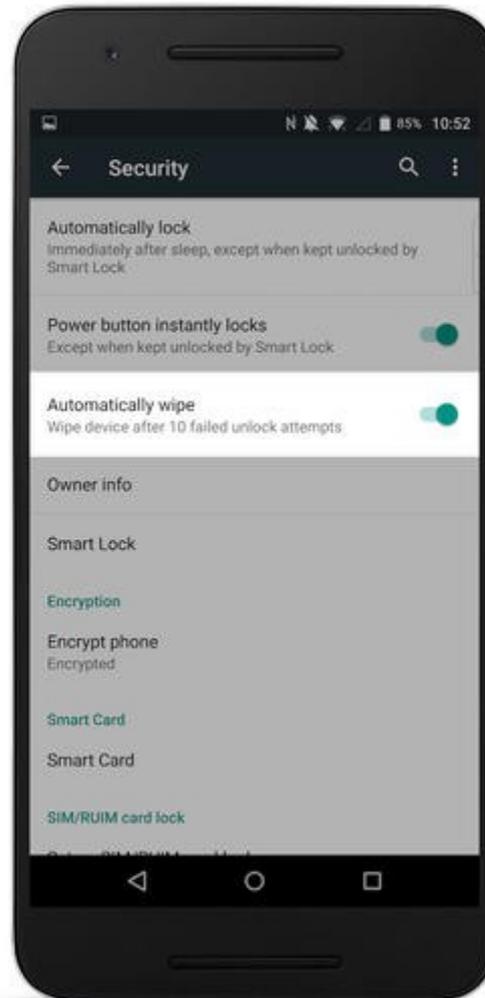
- Ad-tracking is one of the most pervasive ways for Google and its partners to track your habits.
- Turning off interest-based ads prevents ad networks from building up a profile on what you like and what you don't, based on your viewing, reading, or other habits
- Go to **Settings -> Google -> Ads -> Opt out of Ads Personalization** which is disabled by default

Google's Location History

- Your location can say a lot about you, such as where you go and even who you meet and what you might do
- Google uses these results to serve more relevant ads and other information. Turning it off can be good for your privacy
- Go to **Settings** then **Location**, where you can turn on and off at the top switch. You can also turn off **Google Location History** by scrolling to the bottom and turning the option off. From here, you can also **Delete Location History** so it gets scrubbed from Google's servers

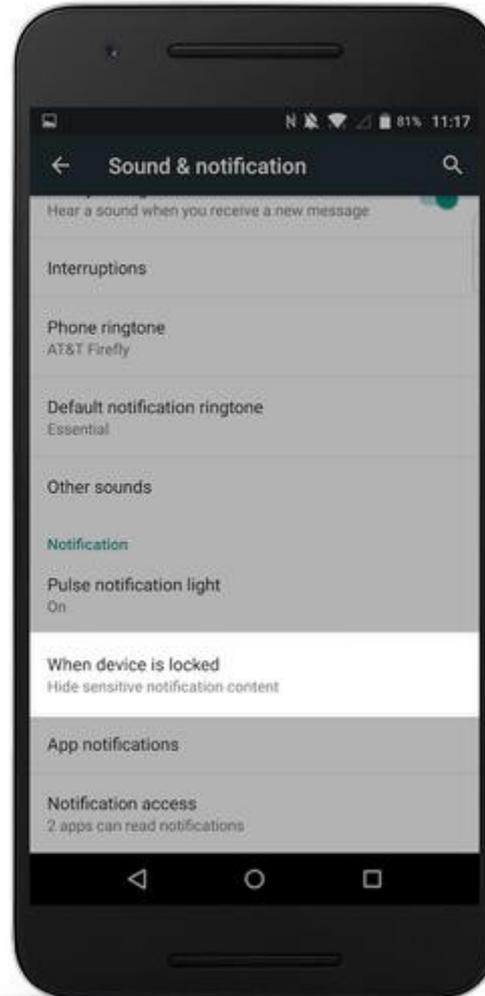


- You can enable a setting so that after ten failed unlock attempts, your Android device will be wiped clean and all data destroyed.
- You can turn this setting on from **Settings** then **Security**, and then (so long as you have your screen lock enabled), you can turn on the **Automatically Wipe** setting -- though, it should be enabled by default



Lock Screen Notifications

- Your lock screen can show a lot about your life.
- Your Android phone or tablet can limit what's shown on the lock screen in order to prevent others' from seeing your personal content as it comes in
- Go to **Settings** then **Sound & Notifications**, and scroll down. You can change how notifications are shown under the **When device is locked** setting. The most privacy conscious setting is to **Hide sensitive notification content** so that you know which app is alerting you, without showing its contents





- Unlike iPhones and iPads, Android devices can run third-party content outside of the Google Play app store.
- This can open up a device to malware attacks.
- The easiest way to ensure that only verified and malware-checked apps can be installed on your phone or tablet is by going to **Settings** then **Security**, and ensuring that the **Unknown sources** option is turned off

- Make sure to keep your Android device up-to-date
- Ensure that Auto-Update is turned on for auto updation of security patches
- Go to **Settings -> Software Update -> Auto Update**



How to protect your Smart Phones

- Always update your devices with the latest software
- Especially, install all security patches provided by the OEMs to patch various security threats
- Never visit any shady websites by clicking on the links you have received over SMS, Whatsapp or by any other means
- Never install apps or software from unfamiliar publishers or from third-party app-stores
- Never use public WiFi hotspots for performing critical transactions

References

- <https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf>
- <https://www.wandera.com/files/mobilethreatlandscape-report2020wpvoebwoncaz/mobile-threat-landscape-report-2020-page-5/>
- <https://www.hindustantimes.com/tech/smartphones-hotspots-of-cyberattacks-in-india-check-point/story-zJQDykref5bqH4IDYFkAMO.html>
- <https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/>
- <https://www.zdnet.com/pictures/android-phone-tablet-privacy-security-settings/15/>



Thank You